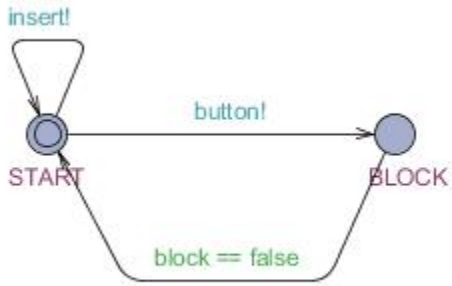
Model 1 검증

한글 명세

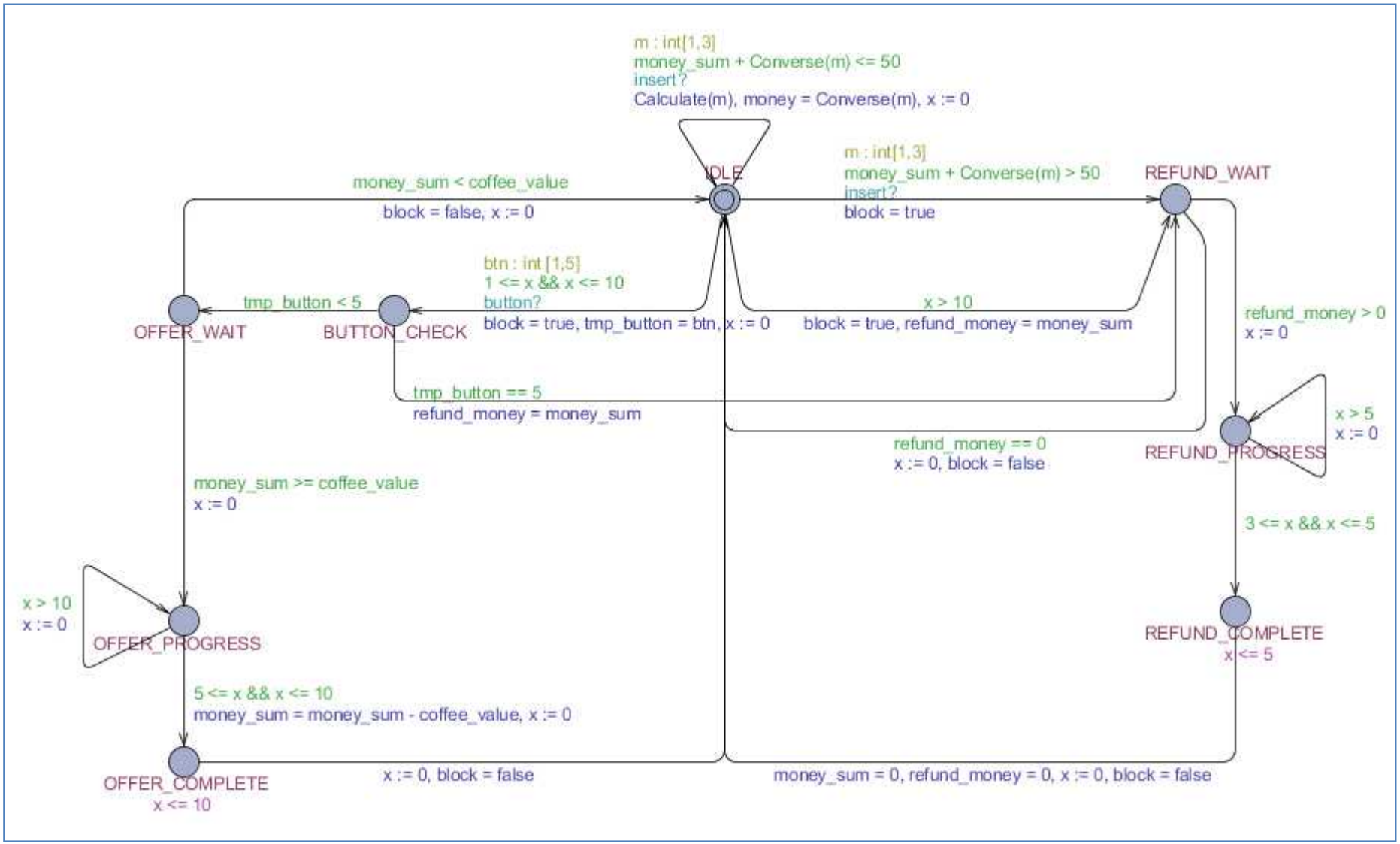
- 한글로 커피 자판기에 필수 요소들을 명시

1. 유저는 금액을 삽입하거나 버튼을 누르는 행위를 할 수 있다. ---------- (0)
2. 유저는 버튼을 누른 후 해당 동작이 완료될 때 까지 다른 작업을 할 수 없다. ----- (0)
3. 버튼은 커피버튼 4개와 환불버튼 1개로 구성된다. ---------- (0)
4. 커피 밴딩 머신은 버튼이 들어오기 전까지 계속해서 금액을 넣을 수 있다. ------- (0)
5. 최대 넣을 수 있는 금액은 5000원이다. ---------- (0)
6. 커피 버튼이 눌리면 10초 이내에 해당 커피를 제공한다. ---------- (0)
7. 커피 버튼이 눌렸을 때 잔액이 충분하지 않으면 해당 작업을 건너뛴다. --------- (0)
8. 10초이내 커피를 제공하지 못할 경우 해당 작업을 다시 시도한다. ---------- (0)
9. 환불 버튼이 눌리면 5초 이내에 잔액을 반환한다. ---------- (0)
10. 돈을 넣은 후 10초 이내 버튼 입력이 들어오지 않으면 5초 이내에 잔액을 반환한다.(0)
11. 최대 넣을 수 있는 금액이 초과되면 초과되는 금액을 5초 이내에 반환한다. ------(0)
12. 5초 이내에 잔액을 반환하지 못하면 반환 작업을 다시 시도한다. ----------(0)

Timed Automata로 구현



Timed Automata로 구현



검증을 위한 Property

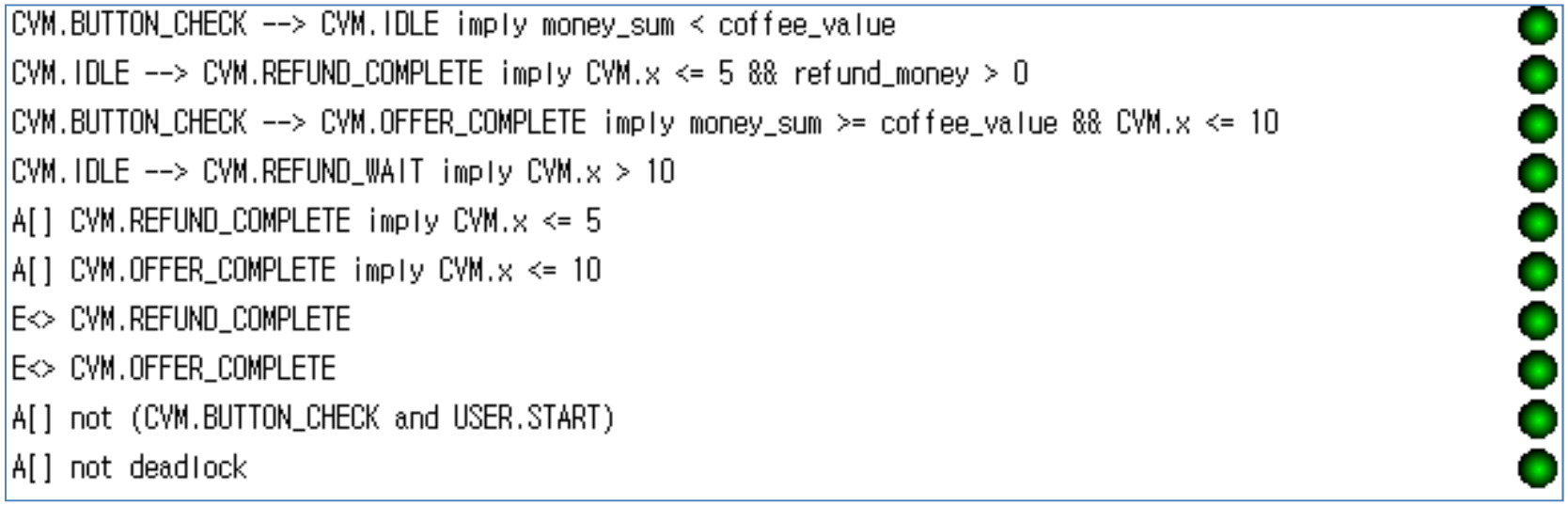
- 우리의 Specification이 만족하는지 여부를 테스트 하기 위한 Property를 만듬
  - 시스템은 데드락 상태에 빠지지 않는다.
  - 버튼이 눌려 있는 상태에서는 동전을 삽입하거나 버튼을 누를 수 없다.
  - 커피자판기는 커피를 제공할 수 있다.
  - 커피자판기는 환불이 가능하다.
  - 항상 10초 이내에 커피가 제공된다.

검증을 위한 Property

- 항상 5초 이내에 환불이 제공된다.
- 항상 10초 동안 버튼 입력이 들어오지 않으면 잔액이 환불 된다.
- 항상 커피 버튼이 눌렸을 때 잔액이 남아 있으면 10초 이내에 해당 커피가 나온다.
- 항상 최대 넣을 수 있는 금액이 초과되면 초과되는 금액을 5초 이내에 반환한다.
- 커피 버튼이 눌렸을 때 잔액이 충분하지 않으면 해당 작업을 건너뛴다.

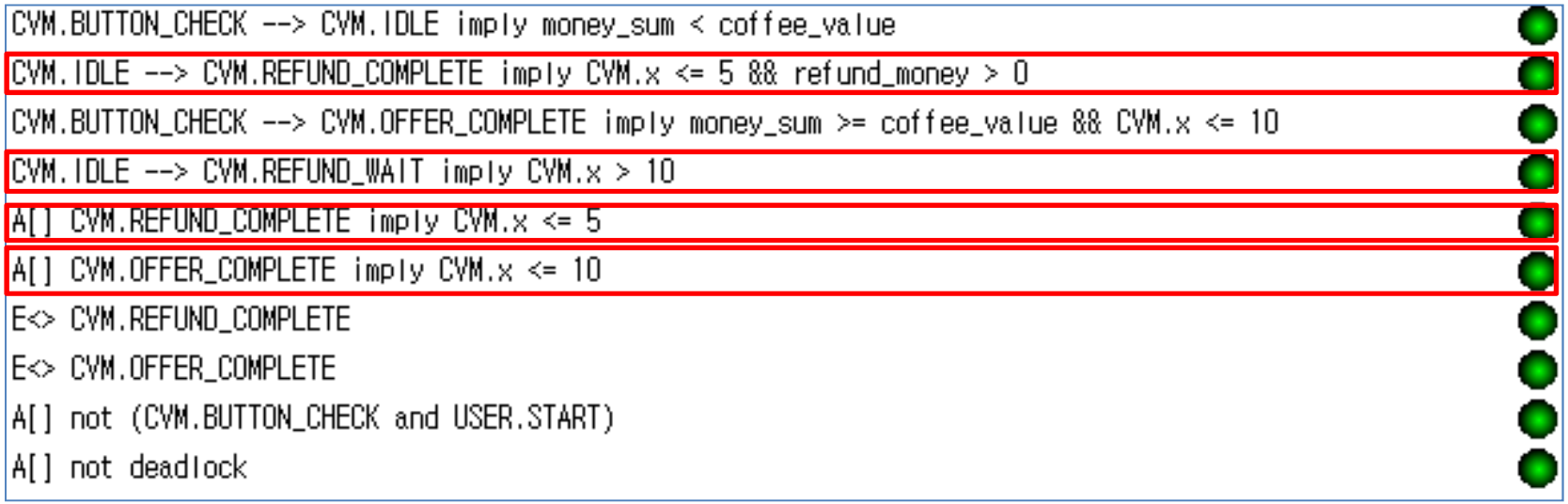
LTL로 Property 변환

- 한글에서 LTL로 Property를 변환

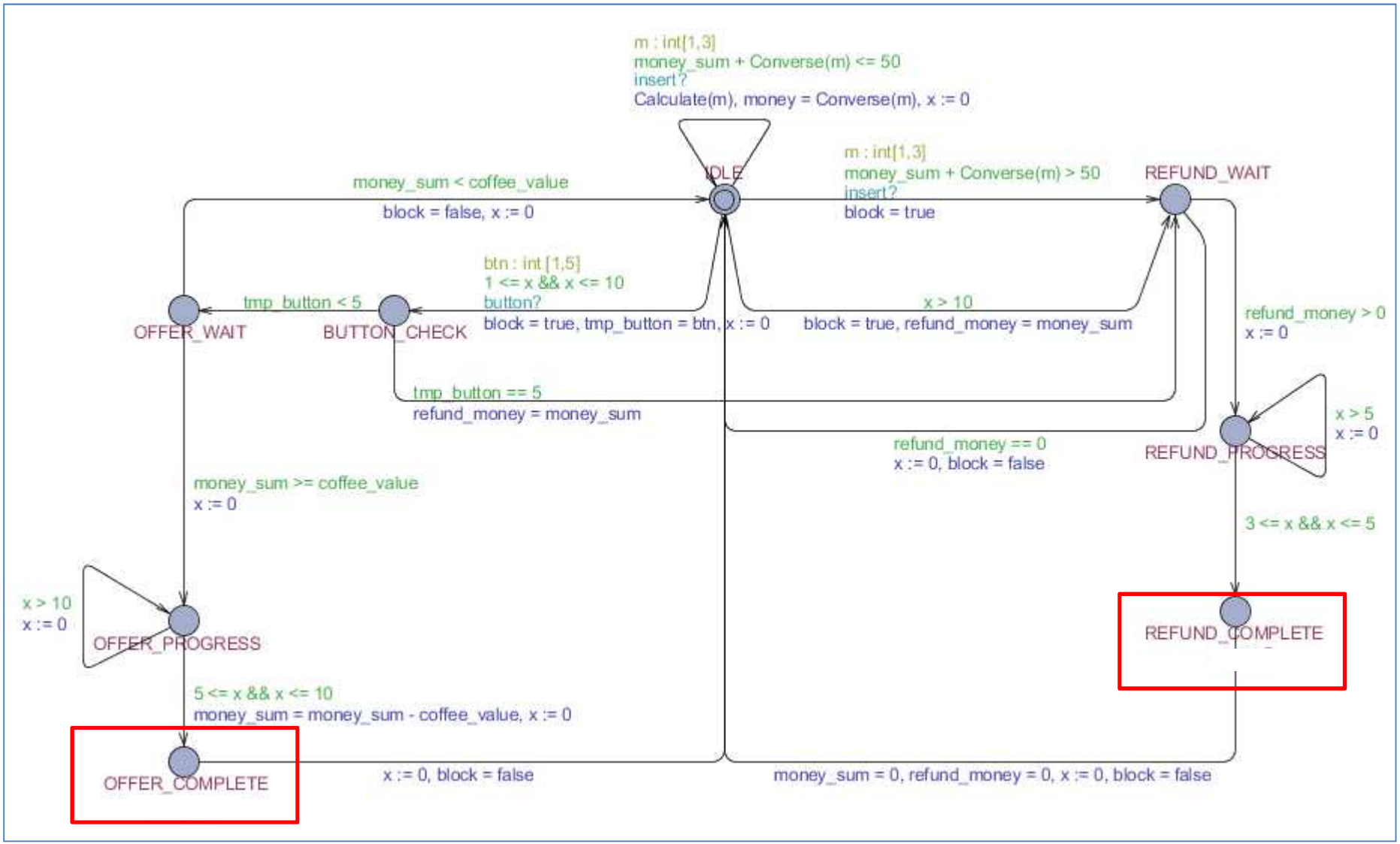


Fail 이 발생한 Property

- 시간과 관련된 Property 들에서 fail 발생



문제가 발생하는 부분


m : int[1,3]
money_sum + Converse(m) <= 50
insert?
Calculate(m), money = Converse(m), x := 0
IDLE
m : int[1,3]
money_sum + Converse(m) > 50
insert?
block = true
REFUND_WAIT
money_sum < coffee_value
block = false, x := 0
btn : int [1,5]
1 <= x && x <= 10
button?
block = true, tmp_button = btn, x := 0
tmp_button < 5
OFFER_WAIT
BUTTON_CHECK
x > 10
block = true, refund_money = money_sum
refund_money > 0
x := 0
tmp_button == 5
refund_money = money_sum
x > 5
x := 0
refund_money == 0
x := 0, block = false
REFUND_PROGRESS
money_sum >= coffee_value
x := 0
3 <= x && x <= 5
x > 10
x := 0
OFFER_PROGRESS
REFUND_COMPLETE
5 <= x && x <= 10
money_sum = money_sum - coffee_value, x := 0
OFFER_COMPLETE
x := 0, block = false
money_sum = 0, refund_money = 0, x := 0, block = false